E-Hub Workshop Results

July 24, 2008

Agenda

- Workshop Objectives
- E-Hub Solution Requirements
- E-Hub Design Options
- Evaluation Criteria
- Solution Evaluation
- Key Issues
- Next Steps

Workshop Objectives

- Understand individual department requirements
- Develop a design concept
  - Secures and protects the State's email
  - Meets individual agency requirements
  - Supports E-mail as a critical service
- Understand barriers to implementation
- Define basic support processes
- Develop migration approach and high level plan
- Scope does not include end-points security, email hosting, archiving, or E-discovery

Requirements – General

- Scope/Scale
  - Scale to 150,000 users
  - Multiple MX records
  - 500K messages per hour
  - Average size-50K
  - Must be Mail platform agnostic (support all SMTP port=25 email traffic)
- Redundancy/Availability
  - Multi- site redundancy
  - Most department require redundant SMTP gateways for high availability
  - Consensus that email is a mission critical service
  - Consensus that email is a 7x24x365/66 service
  - 99.9% availability (include planned maintenance.)
-

Requirements/Features – Mail Hygiene

- **Performance/Capacity**
  - Email in general require minimal latency < 2 minutes
  - There are some needs for shorter latency for certain functions which may requires per domain queuing

- **Anti-spam**
  - Inbound recipient verification
  - Block by attachment size limits
  - Block attachment (by type, policy, fingerprinting, content, encryption)
  - Spam best practice performance requirements
  - Process inter departmental (AV, SPAM) processed through same engine
  - Bi-directional spam
  - Disposition options determined by agency

Requirements/Features – Mail Hygiene

- **Anti-Virus**
  - Scan inbound and outbound and inter- department for viruses
  - 100% accuracy on known virus
  - Advanced protection against zero day attack

- **Message Security**
  - TLS Encryption (gateway to gateway)
  - Capability to enable end-to-end encryption for specific groups of users
    - Agency administered
  - Previously encrypted traffic allowed to pass through from trusted source subject to further review

Requirements/Features – Mail Hygiene

- Content Filtering
  - Filter/block/encrypt/audit on compliance content (by user/group)
    - HIPAA
    - Personal identifiable information (SSN, Drivers license)
    - Payment card Industry (PCI)
    - Medical Requirements
    - Meet federal and State applicable requirements for privacy
    - Configurable by agency or department
- Administration
  - Agency administrator access to quarantine (configurable)
  - Delegated administration
  - Administer disposition granularity (system, department, user, etc.)
  - Access method (http/https)
  - Message store/processing must be hosted in USA – no foreign country hosting (needs further review of State law)

Requirements/Features – Mail Hygiene

- **Reporting**
  - Granularity (by domain, roll-up, by user group)
  - Types of report
    - Capacity and utilization by domain, groups, etc.
    - SPAM efficiency
    - Real time reports
  - Ability to customize report
  - Automatic reporting (scheduled reports)
  - Admin access log reports
  - Admin Log record retention configurable by agency
- **Troubleshooting**
  - Message tracking/trace tools and access to gateway by agency administrators
  - Real time view and monitoring of traffic queues/logs
  - Vendor must be able to detect mail loops

Operational Management

- **Incident Management**
  - 7x24x365 service desk
  - Defined vendor/agency process for incident management

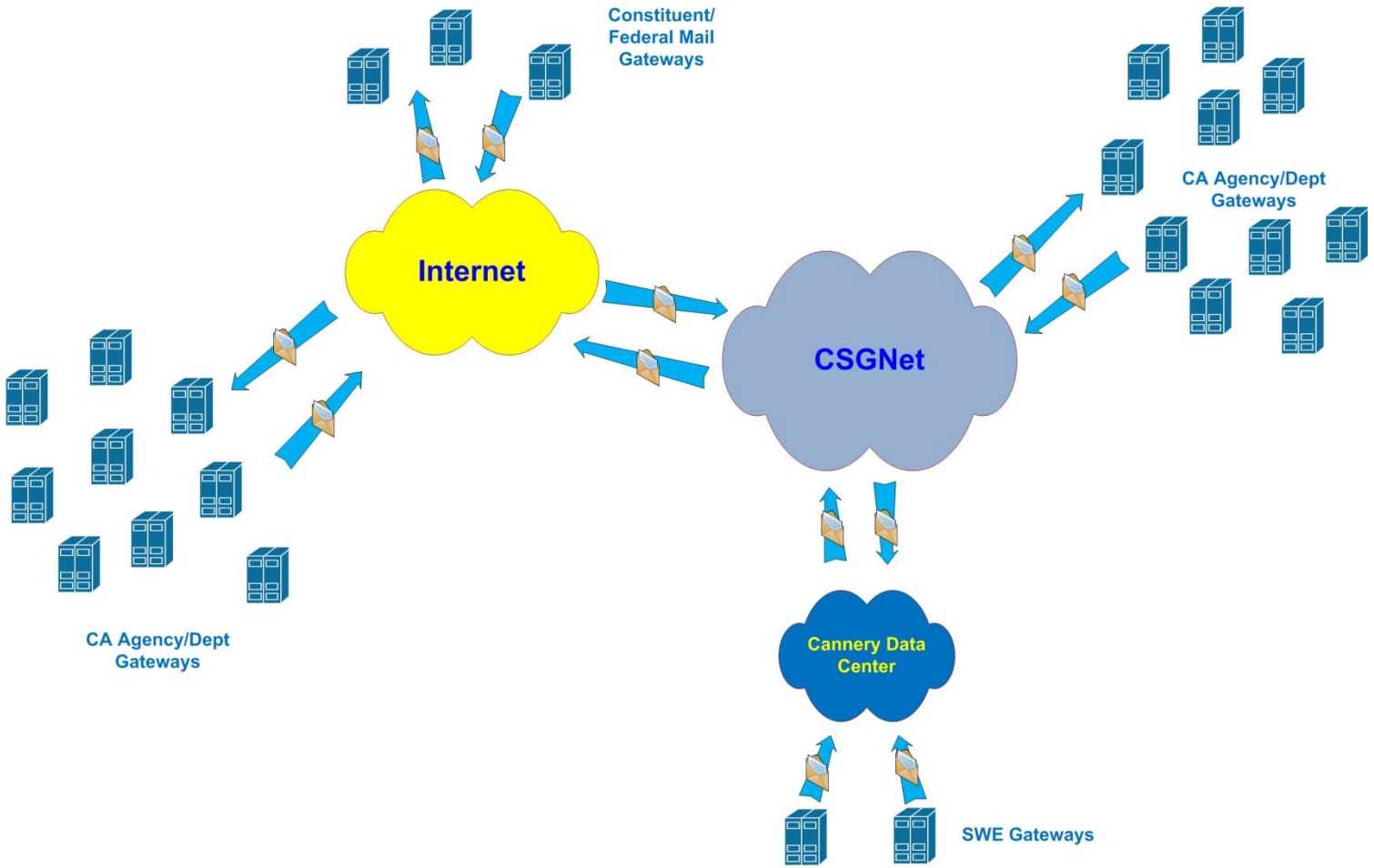
- **Network Management Integration**
  - Configurable threshold alerting
  - Formal notification process

Implementation Requirements

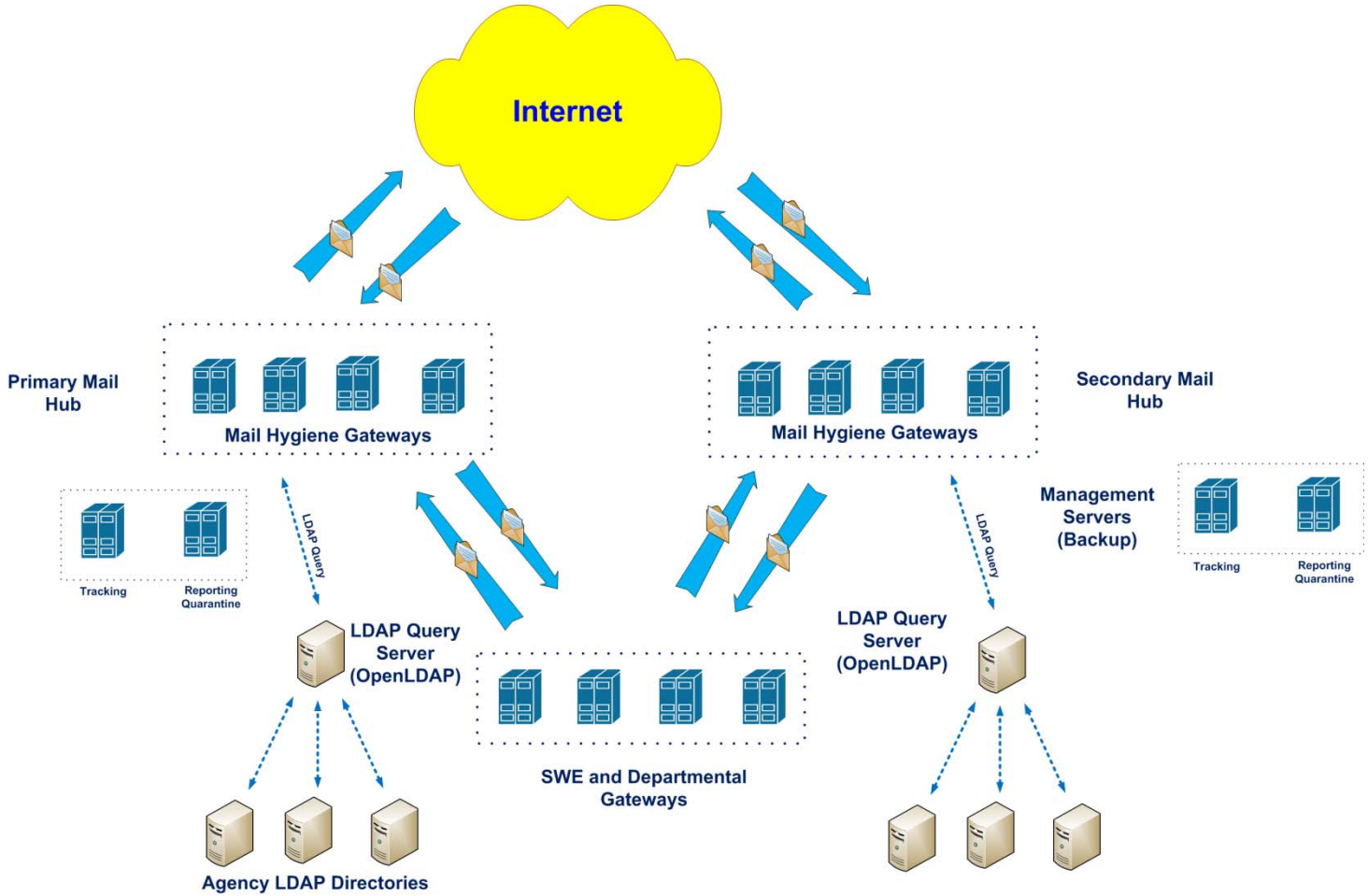
- **Implementation Strategy**
  - Proof of concept/pilot
    - Operation Process design and support structure and documentation
    - Configuration and system documentations
  - Department by department transitions
    - Department gateway changes and coordination
    - Decommission of MTA
    - Time to implementation

- **Implementation Requirements**
  - Training requirements
    - End user (150,000)
    - Administration (500)
  - Directory synchronization (110 directories)
  - Secure connection (TLS, IPSec VPN,..)
    - 110 connections

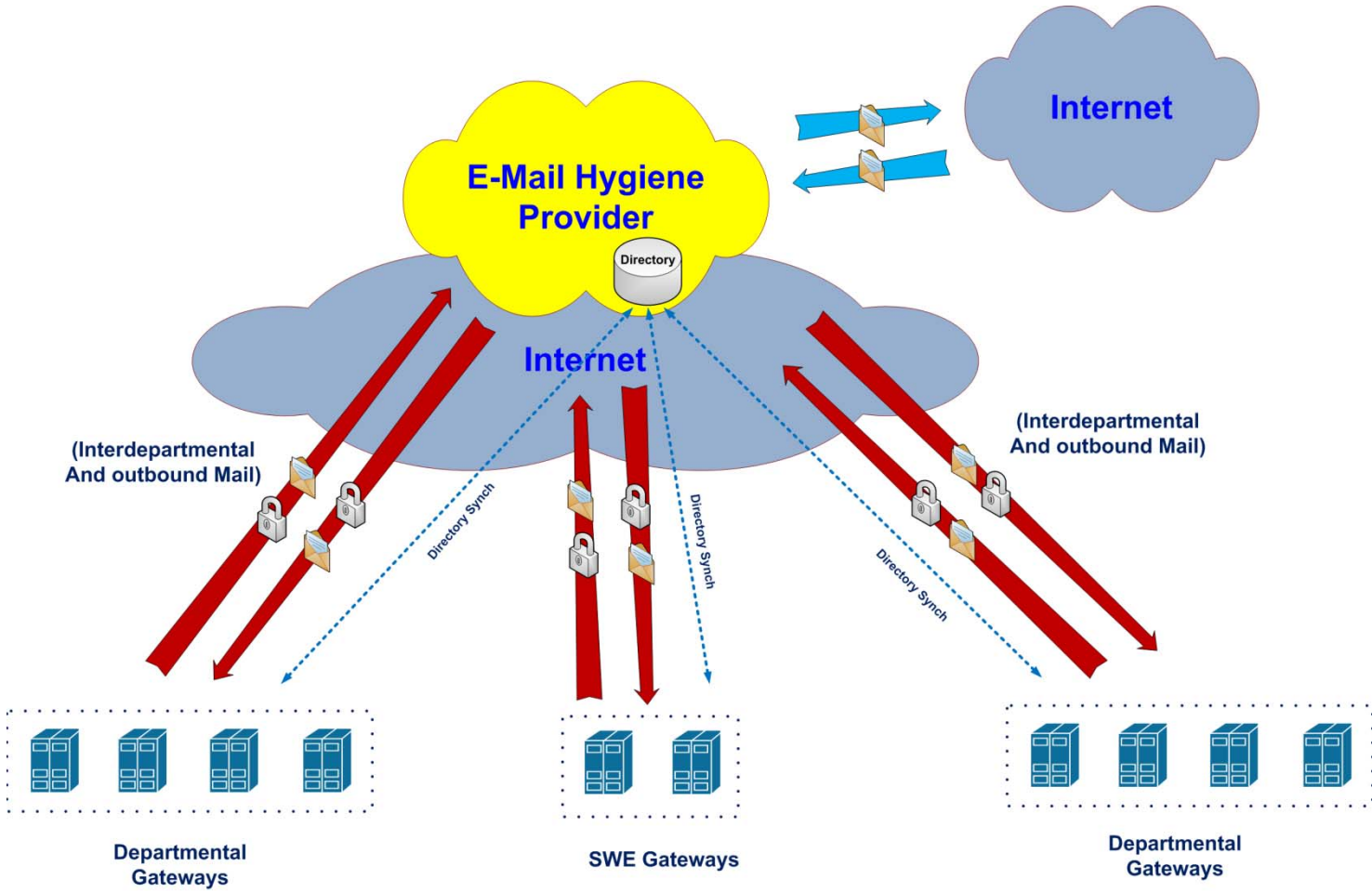
Existing Environment



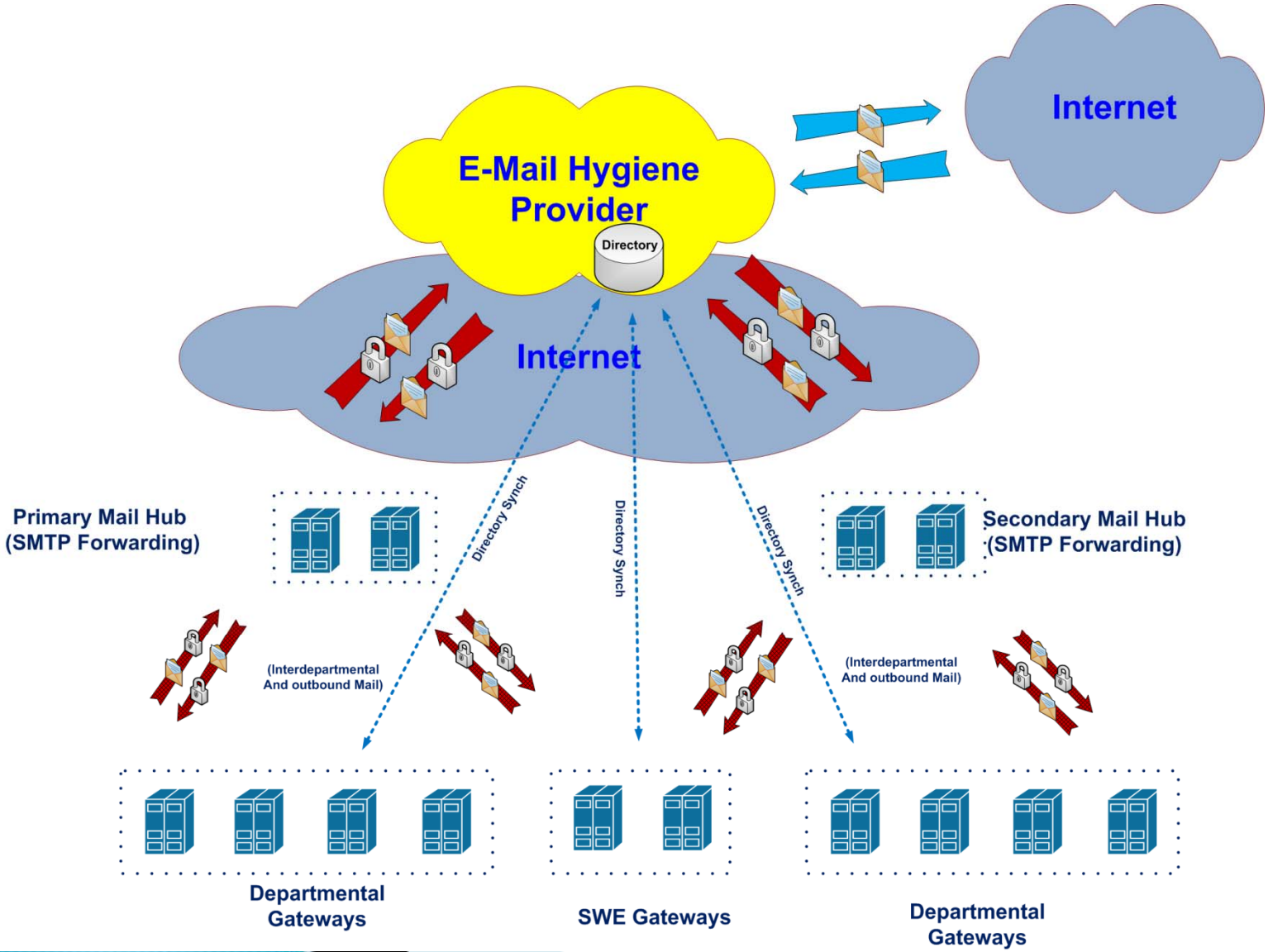
Private Design Topology



Cloud Design Topology



Blended Design (Topology)



Hybrid Solution

- Thumbs Down
  - Complexity
  - Cost
  - Staffing/Resourcing
  - Troubleshooting

Private Solution – Thumbs Down

- Pro's
  - Full control of operations and design
  - Provider executive influence
  - Easier troubleshooting
  - Know who to blame
- Cons
  - Agency doesn't have full control
  - Initial capital cost and licensing
  - Locked into vendor for lifecycle
  - Resources necessary to implement
  - State staffing required to support
  - Locations/facilities

Cloud Solution

- Thumbs Up with Concerns
  - Product specifics
  - Demonstrated Execution – POC
  - Reliable architecture
  - Input to vendor SLAs

Cloud Solution

- Pros
  - Flexibility – not locked in long term to a vendor
  - Appears to scale easily
  - Quick implementation
  - Simple to migrate
  - License as you go
  - No capital outlay
  - Financially backed SLAs
  - Increased services to small agencies
- Cons
  - Possible content filtering limitations
  - Availability during internet outage
  - New concept, new to this group
  - No choke point for traffic sniffing/interception
  - Data and user info stored at remote location

Parking Lot Issues

- Web Based Email (Google, Yahoo, etc.)
- Clarify vendor support for encryption
- Interdepartmental attachment filtering policies

Next Steps

- Draft meeting summary document
- AIO/CIO Presentation of meeting outcome
- Determine best procurement approach